

ELECTRONIC AUTHENTICATION SYSTEM AND ELECTRONIC AUTHENTICATION METHOD

Patent number: JP2003198539

Publication date: 2003-07-11

Inventor: MIYAHARA SHINICHIRO; SHIBATA KOICHI

Applicant: SEIKO INSTR INC

Classification:

- international: G09C1/00; H04L9/32; G09C1/00; H04L9/32; (IPC1-7): H04L9/32; G06F17/60; G09C1/00

- european:

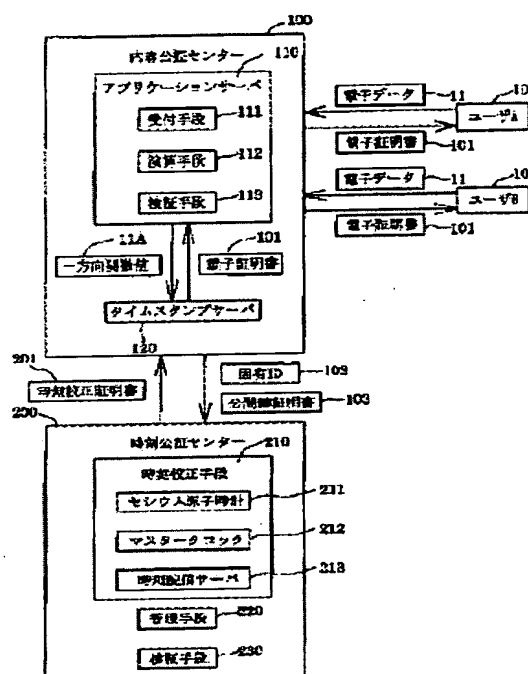
Application number: JP20010396856 20011227

Priority number(s): JP20010396856 20011227

Report a data error here

Abstract of JP2003198539

PROBLEM TO BE SOLVED: To provide an electronic authentication system and an electronic authentication method in which reliability of time stamp information is improved.



Data supplied from the *esp@cenet* database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-198539

(P2003-198539A)

(43) 公開日 平成15年7月11日 (2003.7.11)

(51) Int.Cl. ⁷	識別記号	F I	テ-リ-ド* (参考)
H 0 4 L 9/32		G 0 6 F 17/60	1 4 0 5 J 1 0 4
G 0 6 F 17/60	1 4 0		5 1 2
	5 1 2		Z E C
	Z E C	G 0 9 C 1/00	6 4 0 D
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 D

審査請求 有 請求項の数10 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2001-396856 (P2001-396856)

(22) 出願日 平成13年12月27日 (2001. 12. 27)

(71) 出願人 000002325

セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬1丁目8番地

(72) 発明者 宮原 慎一郎

千葉県千葉市美浜区中瀬1丁目8番地 セ
イコーインスツルメンツ株式会社内

(72) 発明者 柴田 孝一

千葉県千葉市美浜区中瀬1丁目8番地 セ
イコーインスツルメンツ株式会社内

(74) 代理人 100096378

弁理士 坂上 正明

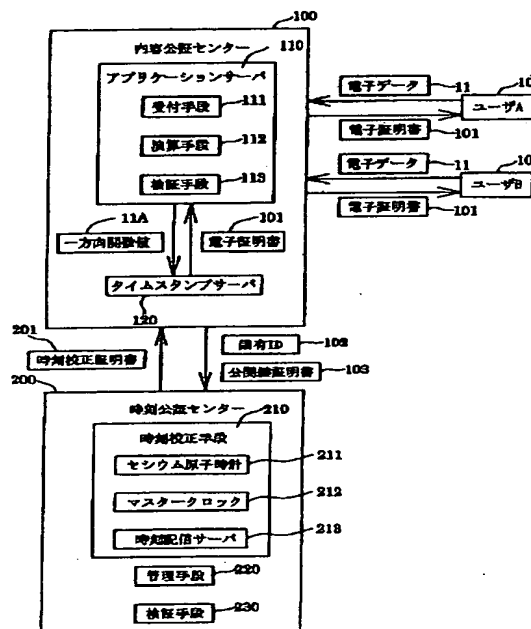
Fターム (参考) 5J104 AA08 EA19 LA01 LA03 LA06
MA03 PA07

(54) 【発明の名称】 電子公証システム及び電子公証方法

(57) 【要約】 (修正有)

【課題】 タイムスタンプ情報の信頼性を向上させた電子公証システム及び電子公証方法を提供する。

【解決手段】 利用者から電子情報の登録を受け付けて電子証明書101を発行すると共に当該電子証明書101に基づいて内容検証を行う内容公証センター100と、前記電子証明書101に基づいて時刻検証を行う独立の時刻公証センター200とを具備する。前記内容公証センター100は、時刻校正されたタイムスタンプ手段120を用いて前記電子証明書101を作成し、前記時刻公証センター200は、時刻校正手段210と、前記タイムスタンプ手段120が固有に使用する秘密鍵と対をなす公開鍵に関する情報を当該タイムスタンプ手段120のIDと共に蓄積する管理手段220と、利用者からの前記電子証明書101に基づいた検証要求を受け付けて前記管理手段220が蓄積した情報に基づいて時刻検証を行う時刻検証手段230とを具備する。



【特許請求の範囲】

【請求項1】 ネットワーク上において電子公証を行う電子公証システムにおいて、

利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを具備し、

前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成し、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行う時刻校正手段と、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段のIDと共に蓄積する管理手段と、利用者からの前記電子証明書に基づいた検証要求を受け付けて前記管理手段が蓄積した情報に基づいて時刻検証を行う時刻検証手段とを具備することを特徴とする電子公証システム。

【請求項2】 前記管理手段は、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のID及び前記特定情報を取得することを特徴とする請求項1に記載の電子公証システム。

【請求項3】 前記管理手段は、前記時刻校正手段が前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする請求項1又は2に記載の電子公証システム。

【請求項4】 前記時刻校正手段は、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイムスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする請求項1～3の何れかに記載の電子公証システム。

【請求項5】 前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする請求項1～4の何れかに記載の電子公証システム。

【請求項6】 ネットワーク上において電子公証を行う電子公証方法において、

利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを設け、

前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成する一方、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行うと共に、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手

段のIDと共に蓄積し、この蓄積情報に基づき、利用者からの前記電子証明書に基づいた検証要求に応じて時刻検証を行うことを特徴とする電子公証方法。

【請求項7】 前記時刻校正センターは、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段のID及び前記特定情報を取得することを特徴とする請求項6に記載の電子公証方法。

【請求項8】 前記時刻校正センターは、前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする請求項6又は7に記載の電子公証方法。

【請求項9】 前記時刻校正センターは、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイムスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする請求項6～8の何れかに記載の電子公証方法。

【請求項10】 前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする請求項6～9の何れかに記載の電子公証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子公証システム及び電子公証方法に関する。

【0002】

【従来の技術】インターネットの普及により、インターネットを介してショッピングや取引を行う電子商取引が一般化され、また、インターネット上で契約を行う必要性が出てきた。

【0003】そこで、電子ネットワーク上で安心して電子商取引や契約を行うことができるために、電子ネットワーク上で公証を行う電子公証システムが出現した。

【0004】電子公証システムは、電子情報について、「いつ、誰が、何を」を登録、照会、証明するシステムである。したがって、電子ネットワーク上の通信を安全に行うための暗号化技術、公開鍵暗号方式を使用した電子署名技術及び正確な時刻を証明するタイムスタンプ技術が必要となる。

【0005】従来の電子公証システムは、図5に示すように行われる。電子公証サービス事業者1は、利用者であるA社2及びB社3等に対して電子公証サービスを提供する。例えば、A社2から電子文書4の登録を受け付け、それに対して電子証明書5を発行する。電子証明書5は、電子文書4の内容から一方関数によって出力される一方関数値、例えば、ハッシュ値、時刻情報およびそれらに対する電子署名等を含むものである。利用者であるA社2とB社3とが電子文書4及び電子証明書5を使用して電子商取引を行う際に、B社3が電子文書4及び電子証明書5を電子公証サービス事業者1へ送信することにより照会を行うと、電子公証サービス事業

は電子文書 4 及び電子証明書 5 の検証を行い、結果を B 社 3 へ通知する。

【0006】

【発明が解決しようとする課題】 上述したような電子公証システムでは、電子文書 4 が登録された時間を証明する電子証明書 5 に含まれる時間情報が正確な時刻であるかどうかについて、疑義が生じる可能性がある。すなわち、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じるという問題がある。

【0007】 本発明は、このような事情に鑑み、タイムスタンプ情報の信頼性を向上させた電子公証システム及び電子公証方法を提供することを課題とする。

【0008】

【課題を解決するための手段】 前記課題を解決する本発明の第 1 の態様は、ネットワーク上において電子公証を行う電子公証システムにおいて、利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを具備し、前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成し、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行う時刻校正手段と、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段の ID と共に蓄積する管理手段と、利用者からの前記電子証明書に基づいた検証要求を受け付けて前記管理手段が蓄積した情報に基づいて時刻検証を行う時刻検証手段とを具備することを特徴とする電子公証システムにある。

【0009】 本発明の第 2 の態様は、第 1 の態様において、前記管理手段は、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段の ID 及び前記特定情報を取得することを特徴とする電子公証システムにある。

【0010】 本発明の第 3 の態様は、第 1 又は 2 の態様において、前記管理手段は、前記時刻校正手段が前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする電子公証システムにある。

【0011】 本発明の第 4 の態様は、第 1 ～ 3 の何れかの態様において、前記時刻校正手段は、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイムスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする電子公証システムにある。

【0012】 本発明の第 5 の態様は、第 1 ～ 4 の何れかの態様において、前記特定情報は、前記タイムスタンプ

手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする電子公証システムにある。

【0013】 本発明の第 6 の態様は、ネットワーク上において電子公証を行う電子公証方法において、利用者から電子情報の登録を受け付けて電子証明書を発行すると共に当該電子証明書に基づいて内容検証を行う内容公証センターと、前記内容公証センターとは独立して存在して前記電子証明書に基づいて時刻検証を行う時刻公証センターとを設け、前記内容公証センターは、前記時刻公証センターが時刻校正するタイムスタンプ手段を用いて前記電子証明書を作成する一方、前記時刻公証センターは、前記タイムスタンプ手段の時刻校正を行うと共に、前記タイムスタンプ手段が固有に使用する秘密鍵と対をなす公開鍵の情報若しくは当該公開鍵を特定するための情報であって前記電子証明書に含まれる特定情報を当該タイムスタンプ手段の ID と共に蓄積し、この蓄積情報に基づき、利用者からの前記電子証明書に基づいた検証要求に応じて時刻検証を行うことを特徴とする電子公証方法にある。

【0014】 本発明の第 7 の態様は、第 6 の態様において、前記時刻校正センターは、ネットワークを介して前記タイムスタンプ手段にアクセスして当該タイムスタンプ手段の ID 及び前記特定情報を取得することを特徴とする電子公証方法にある。

【0015】 本発明の第 8 の態様は、第 6 又は 7 の態様において、前記時刻校正センターは、前記タイムスタンプ手段の時刻校正を行う際に前記特定情報を取得することを特徴とする電子公証方法にある。

【0016】 本発明の第 9 の態様は、第 6 ～ 8 の何れかの態様において、前記時刻校正センターは、時刻校正を行う際に時刻校正証明書を前記タイムスタンプ手段に送信し、当該タイムスタンプ手段は、この時刻校正証明書を含めて前記電子証明書を発行することを特徴とする電子公証方法にある。

【0017】 本発明の第 10 の態様は、第 6 ～ 9 の何れかの態様において、前記特定情報は、前記タイムスタンプ手段が使用する秘密鍵と対をなす公開鍵の公開鍵証明書であることを特徴とする電子公証方法にある。

【0018】 かかる本発明では、電子情報についての電子証明書に基づいて内容検証を行う内容公証センターと、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じることなく、タイムスタンプ情報の信頼性を向上させることができる。

【0019】

【発明の実施の形態】 以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【0020】 図 1 には、一実施形態に係る電子データ公証システムの概要を示す。同図に示すように、本実施形

態の電子データ公証システムは、内容公証センター 100 及び時刻公証センター 200 が対となって電子データの内容及び時刻の公証サービスをユーザ A、ユーザ B 等のユーザ 10 に提供するものであり、一つの時刻公証センター 200 に対して複数の内容公証センター 100 が存在し、サービスを提供することができる。なお、内容公証センター 100 及び時刻公証センター 200 とは、相互に独立した主体が管理するのが好ましい。また、各ユーザ 10 は、名称又は氏名、固有 ID の他、電子署名および署名に用いる公開鍵証明書等を、事前に内容公証センター 100 及び時刻公証センター 200 へ登録するのが好ましい。これにより、公証をスムーズに行うことができ、また、ユーザ 10 と内容公証センター 100 との通信を全て署名・暗号化して行うことができ、通信段階での改ざん、盗聴、成りすまし等を防止することができる。

【0021】ここで、ユーザ 10 は、電子データ 11 を内容公証センター 100 へ送信することにより、その電子データ 11 の内容及び時刻を公証するための電子証明書 101 を受信することができる。なお、ユーザ 10 は、好ましくは、予め、内容公証センター 100 に登録した電子署名を用いて電子データ 11 を暗号化して送信するようにするのが好ましい。

【0022】一方、内容公証センター 100 は、ユーザ 10 から公証の受付及び検証を行うアプリケーションサーバ 110 を有し、アプリケーションサーバ 110 は、ユーザ 10 からの受付及びユーザ 10 への電子証明書 101 の送信を行う受付手段 111 と、受け付けた電子データ 11 を受信して電子証明書 101 を作成するための一方向関数値を作成する演算手段 112 と、ユーザ 10 からの検証要求に対応する検証手段 113 とを具備する。また、内容公証センター 100 は、一方向関数値にタイムスタンプ情報を付与して電子証明書 101 を発行するタイムスタンプサーバ 120 を具備する。

【0023】ここで、受付手段 111 は、ユーザ 10 からの接続要求を受け付け、ユーザ 10 の固有 ID などの必要な情報を受信すると共に、電子データ 11 を受信する。なお、電子データ 11 が暗号化されている場合には、復号すると共に電子署名により改ざん等が無いことを検証する。

【0024】演算手段 112 は、受付手段 111 が受信した電子データ 11 から一方向関数値を作成し、タイムスタンプサーバ 120 に渡す。ここで、一方向関数値とは、例えば、ハッシュ (HASH) 値、メッセージダイジェストとも呼ばれるもので、ハッシュ関数などの不可逆な一方向関数により生成された、例えば、固定長の疑似乱数である。同一のデータからは同一の一方向関数値が得られるが、一方向関数値から元のデータを再現することはできない。

【0025】検証手段 113 は、ユーザ 10 からの電子

データ 11 及びそれに対する電子証明書 101 と共に検証要求を受け付け、これらに対する改ざん等がないことを検証するもので、詳細は後述する。

【0026】タイムスタンプサーバ 120 は、演算手段 112 から一方向関数値を受け取り、これにタイムスタンプ情報を付加して電子証明書 101 を作成するものであれば特に限定されない。また、電子証明書 101 は、所定の手順により暗号化・署名されているのが好ましく、タイムスタンプサーバ 120 により使用される時刻情報は、時刻公証センター 200 により定期的に校正されている。なお、これらの点に付いて詳細は後述する。

【0027】タイムスタンプサーバ 120 の時刻校正を行う時刻公証センター 200 は、時刻校正手段 210 を具備し、時刻校正手段 210 は、例えば、協定世界時と協調するセシウム原子時計 211、セシウム原子時計 211 から時刻ソースが供給されるマスタークロック 212 及びマスタークロック 212 から時刻配信される時刻配信サーバ 213 とを具備し、時刻配信サーバ 213 がタイムスタンプサーバ 120 の時刻手段を定期的に校正する。

【0028】ここで、時刻公証センター 200 は、定期的にタイムスタンプサーバ 120 にアクセスし、内蔵される時計の校正を行うと共に、タイムスタンプサーバ 120 の固有 ID 102 及び当該タイムスタンプサーバ 120 が使用する公開鍵の公開鍵証明書 103 を取得し、当該公開鍵証明書 103 の一方向関数値であるハッシュ値を含む時刻校正証明書 201 を発行する。

【0029】また、時刻公証センター 200 は、各タイムスタンプサーバ 120 の固有 ID 102 と共に当該タイムスタンプサーバ 120 が使用する公開鍵を特定する情報を蓄積して管理する管理手段 220 と、ユーザ 10 からの電子データ 11 及びそれに対する電子証明書 101 と共に検証要求を受け付け、これらに対する改ざん等がないことを検証する検証手段 230 とを具備する。ここで、タイムスタンプサーバ 120 が使用する公開鍵を特定する特定情報としては、時刻校正手段 210 がタイムスタンプサーバ 120 の時刻公証を行う際に取得する公開鍵証明書 103 を挙げるができるが、これに限定されず、タイムスタンプサーバ 120 が使用する公開鍵を別途取得して蓄積してもよい。

【0030】このようなタイムスタンプサーバ 120 の一例及びこのタイムスタンプサーバ 120 により発行される電子証明書 101 の一例を図 2 に示す。図 2 に示すように、タイムスタンプサーバ 120 は、時刻公証センター 200 により管理された固有 ID 102 を有すると共に時計 121 を内蔵し、電子証明書作成手段 122 を具備する。また、電子証明書 101 を作成する際に暗号化に使用する秘密鍵 123 及びこの秘密鍵 123 と対をなす公開鍵の公開鍵証明書 103 を有する。また、タイムスタンプサーバ 120 の時計 121 は、上述したよう

に、時刻公証センター 200 の時刻校正手段 210 により定期的に所定のタイミングで校正されており、この校正時に時刻校正証明書 201 を受信し、これを保管している。なお、時刻公証センター 200 は、時刻校正時にタイムスタンプサーバ 120 から固有 ID 102 及び公開鍵証明書 103 を取得し、これにより、当該タイムスタンプサーバ 120 が適正な電子証明書 101 を生成しているかどうかを監視し、発行した電子証明書 101 について認証する。

【0031】電子証明書作成手段 122 は、ユーザ 10 の電子データ 11 の一方向関数値 11A を演算手段 112 から受信してこれに時計 121 から取得した時刻情報を付加したタイムスタンプ情報 104 を作成すると共に、このタイムスタンプ情報 104 を秘密鍵 123 で暗号化すると共に署名した電子署名 105 を作成し、電子証明書 101 として出力する。従って、電子証明書 101 は、タイムスタンプ情報 104 及び電子署名 105 を具備し、さらに、タイムスタンプ用秘密鍵の公開鍵証明書 103 及び時刻校正証明書 201 を含むものである。

【0032】このような電子証明書 101 の使用例を図 3 に示す。図 3 に示す例では、電子証明書 101 を内容公証センター 100 から取得したユーザ 10 (ユーザ A) が、電子データ 11 と共に電子証明書 101 をユーザ 20 (ユーザ X) に対して使用し、ユーザ 20 が電子データ 11 及び電子証明書 101 を使用して内容検証要求 301 を行う場合を想定している。ここで、ユーザ 20 は、電子データ 11 及び電子証明書 101 を用いて内容公証センター 100 へ内容検証要求 301 を行うことにより、電子データ 11 の改ざん、日付の変更等がないことを内容証明 302 により確認することができる。一方、ユーザ 20 は、電子証明書 101 を用いて時刻公証センター 200 へ時刻検証要求 303 を行うことにより、内容公証センター 100 が時刻公証センター 200 による時刻校正を受けている正規のタイムスタンプサーバ 120 を使用しており、電子証明書 101 が正規のタイムスタンプサーバ 120 が発行したものであることを、時刻証明 304 により確認することができる。すなわち、ユーザ 20 は、電子情報のやりとりだけで、電子情報の改ざん等による不正を看破することができる。

【0033】ここで、内容公証センター 100 が内容証明 302 を行う手段、並びに時刻公証サーバ 200 が時刻証明 304 を行う手段については特に限定されず、ユーザ 20 に対して証明書を発行してもよいし、電子メール等で連絡してもよいし、ユーザ 20 がウェブ上で確認できるようにしてもよい。

【0034】また、内容公証センター 100 は、検証手段 113 が、例えば、ユーザ 20 から受信した電子データ 11 から上述した演算手段 112 と同様にハッシュ値を求め、これと、電子証明書 101 のタイムスタンプ情報 104 に含まれるハッシュ値と一致するかどうかを検

証することにより、内容証明 302 を行う。勿論、検証手段 113 は、電子データ 11 の内容のみの検証ではなく、すなわち、内容に改ざん等があるか否かの検証だけでなく、タイムスタンプ情報に改ざん等があるか否かの検証をも行うものである。

【0035】一方、時刻公証センター 200 の検証手段 230 が時刻証明 304 を行うまでの手順は図 4 に示す通りである。すなわち、ユーザ 20 から電子証明書 101 と共に時刻検証要求 303 を受けると、受信した電子証明書 101 のタイムスタンプ情報 104 に含まれているタイムスタンプサーバ 120 の固有 ID 102 と、時刻校正証明書 201 を作成した際に使用した公開鍵証明書 103 とを含む検証情報 106 を取得する。この検証情報 106 が、管理手段 220 が蓄積した固有 ID 102 及び公開鍵証明書 103 を含むデータベース 221 に含まれるか否かを検証し、含まれることを条件として時刻証明 304 を行う。ここで、時刻証明 304 は、内容証明 302 のように電子証明書 101 に改ざん、不正があるか否かではなく、電子証明書 101 が、時刻公証センター 200 により所定の時刻校正を受けて管理されているタイムスタンプサーバ 120 により発行された真正なものであることを証明するものである。

【0036】通常、時刻校正証明書 201 が真正なものかどうかを検証することにより、電子証明書 101 を真正なものとなすことができるが、時刻校正証明書 201 自体を模倣・複製することも考えられるので、タイムスタンプ情報 104 に含まれる固有 ID 102 と時刻校正証明書 201 を作成した際に使用した公開鍵証明書 103 との対により、正規のタイムスタンプサーバ 120 が発行したものか否かを検証するようにしている。また、時刻校正証明書 201 を検証することにより、当該電子証明書 101 を発行したタイムスタンプサーバ 120 が現在でも定期的に時刻校正を受けているかを把握することができ、これにより、電子証明書 101 に含まれるタイムスタンプ情報 104 が正確か否かの判断を行うことができる。さらに、このような検証を行うことにより、偽の固有 ID 及び公開鍵証明書を保有した偽のタイムスタンプサーバが発行した電子証明書も看破することができる。

【0037】以上説明したように、電子情報についての電子証明書に基づいて内容検証を行う内容公証センターと、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、時刻検証については必要に応じて二重に検証することができ、タイムスタンプ情報の信頼性を向上させることができるので、タイムスタンプ情報が重視された新しい使用態様に対応することができる。

【0038】

【発明の効果】本発明によれば、電子情報についての電子証明書に基づいて内容検証を行う内容公証センター

と、電子証明書に基づいて時刻検証を行う時刻公証センターとを独立させることにより、正確な時刻をタイムスタンプされているか？改ざんされた時刻ではないか？などの疑問が生じることなく、タイムスタンプ情報の信頼性を向上させることができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る電子データ公証システムの概略構成例を示す図である。

【図2】本発明の一実施形態におけるタイムスタンプサーバ及び電子証明書を説明する図である。

【図3】本発明の一実施形態における電子証明書の使用態様を表す図である。

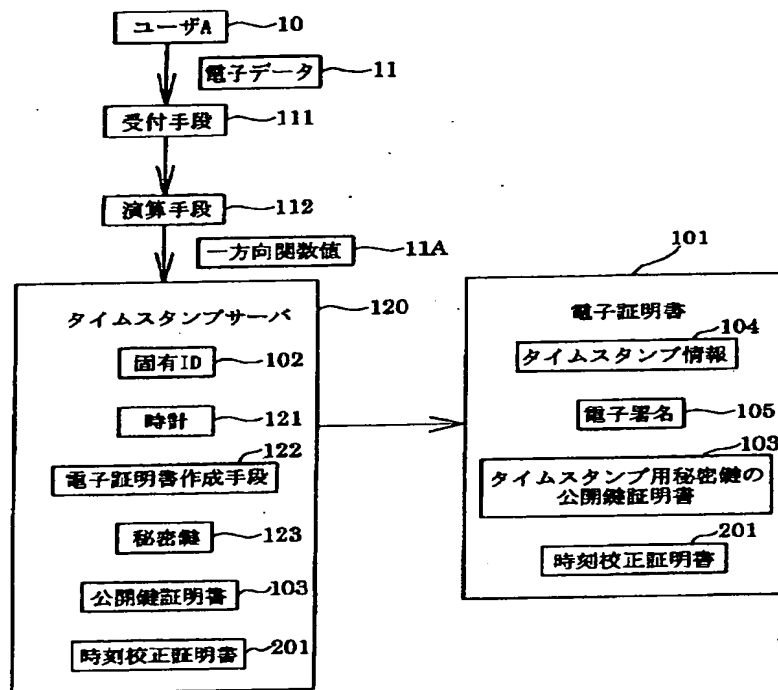
【図4】本発明の一実施形態に係る時刻証明の手順を説明する図である。

【図5】従来技術に係る電子公証システムの概略構成例を示す図である。

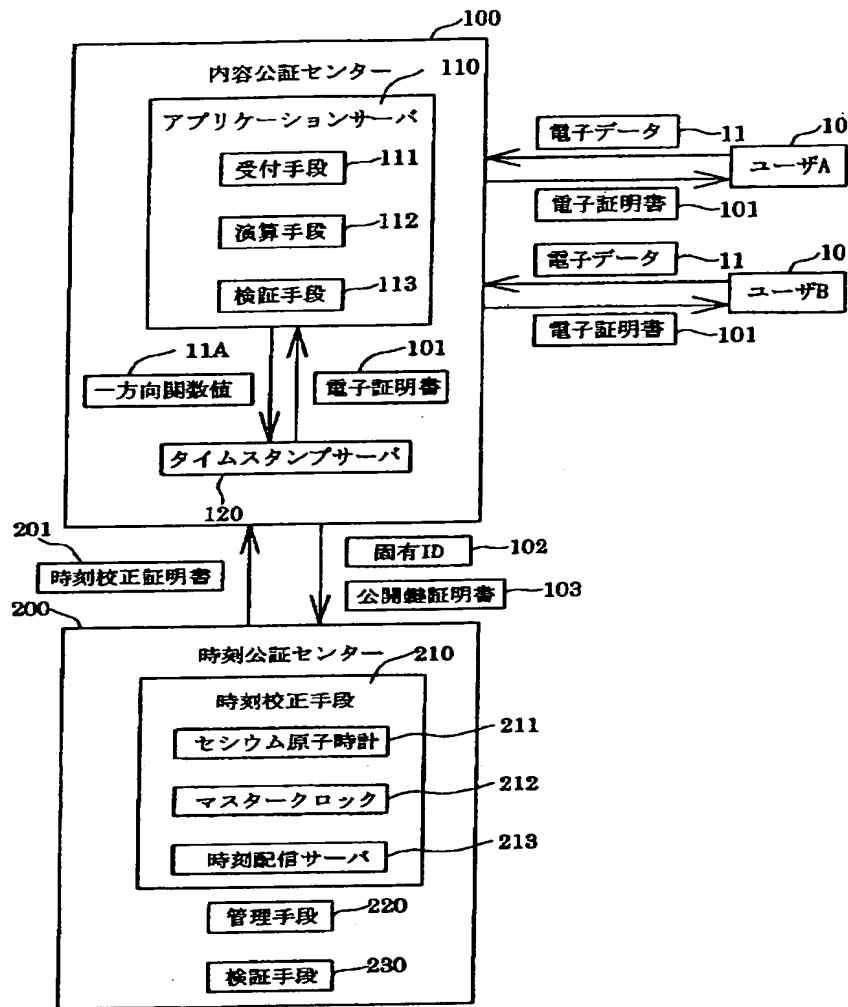
【符号の説明】

- * 10 ユーザA、ユーザB
- 20 ユーザX
- 11 電子データ
- 11A 一方向関数値
- 100 内容公証センター
- 101 電子証明書
- 102 固有ID
- 103 公開鍵証明書
- 110 アプリケーションサーバ
- 10 111 受付手段
- 112 演算手段
- 113 検証手段
- 120 タイムスタンプサーバ
- 200 時刻公証センター
- 210 時刻校正手段
- 220 管理手段
- * 230 検証手段

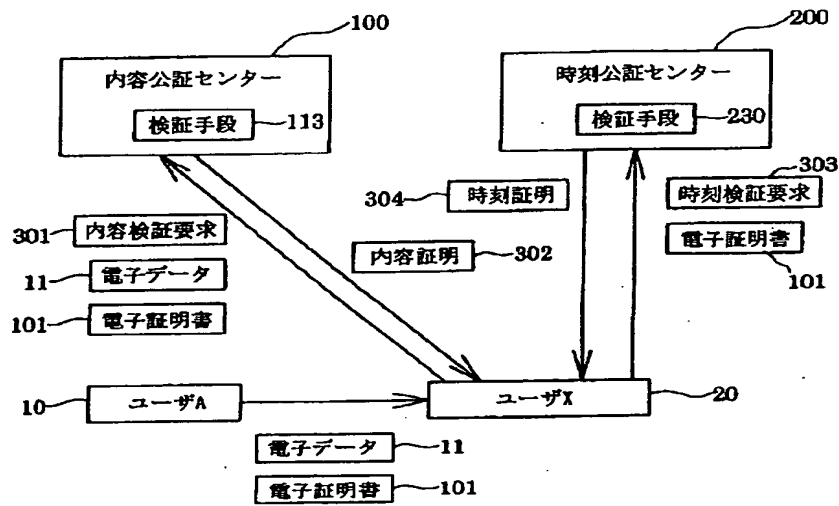
【図2】



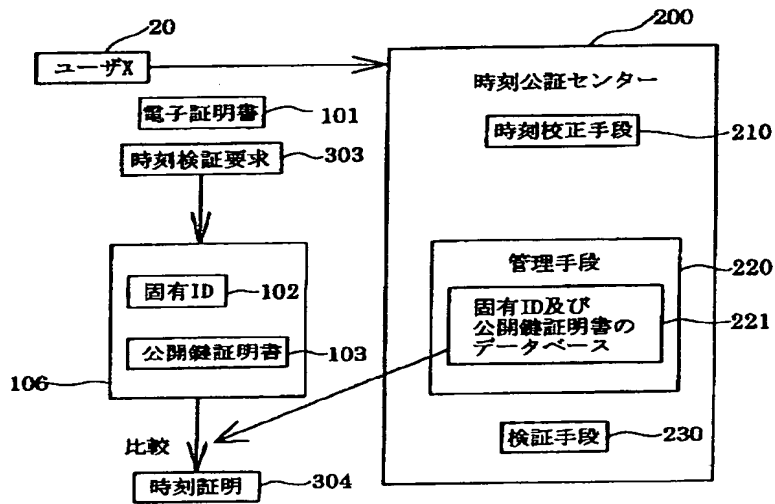
【図1】



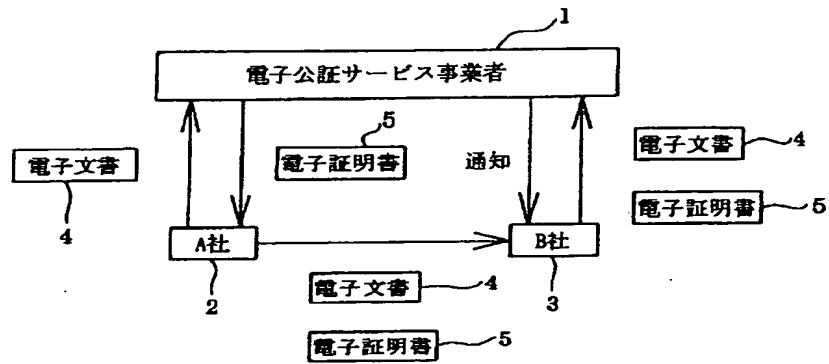
【図3】



【図4】



【図5】



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I
H 0 4 L 9/00

テーマコード(参考)

6 7 5 B